Security Vulnerability Self-Assessment

Guide for Critical Infrastructure Protection

Utah Department of Public Safety
Division of Homeland Security

www.des.utah.gov
www.BeReadyUtah.gov

August 2006

A Note about Security for this Document

This document contains sensitive information about the security of your infrastructure. Therefore, it should be treated as ***Confidential Information*** *and should be stored in a secure place in the organization. A duplicate copy should also be stored in a secure off-site location.*

Contents

Security Vulnerability Self-Assessment Guide

Introduction

Infrastructures are critical to every community. Protection of those infrastructures must be a high priority for private and public officials to ensure an uninterrupted service, which is essential for the protection of public safety.

Adequate security measures will help prevent loss of service through terrorist acts, vandalism, or pranks. If your infrastructure is prepared, such actions may even be prevented. The appropriate level of security is best determined at the local level.

This Security Vulnerability Self-Assessment Guide is designed to help you determine possible vulnerable components and identify security measures that should be considered. A “vulnerability assessment” is the identification of weaknesses in infrastructure security, focusing on defined threats that could compromise its ability to provide adequate services. This document is meant to encourage you to review your infrastructure vulnerabilities, but it may not take the place of a comprehensive review by security experts. The Self-Assessment Guide has a simple design. Answers to assessment questions are “yes” or “no,” and there is space to identify needed actions and actions you have taken to improve security.

How to Use this Self-Assessment Guide

This document is to be used by personnel within the organization. Physical facilities pose a high degree of exposure to any security threat. This self-assessment should be conducted on all components of your infrastructure.

The Assessment includes an emergency contact list for your use. This list will help you identify who you need to contact in the event of an emergency or threat and will help you develop communication and outreach procedures. Filling out the Emergency Contact List is an important step toward developing an Emergency Response Plan, which provides detailed procedures on how to respond to an emergency.
You may obtain sample Emergency Response Plans from the Division of Homeland Security.

Security is everyone’s responsibility. We hope this document helps you to increase the awareness of all your employees, governing officials, and customers about security issues. Once you have completed this document, review the actions you need to take to improve your infrastructure’s security. Make sure to prioritize your actions based on the most likely threats. Please complete the Certificate of Completion on page 25 and return only the certificate to the Division of Homeland Security Critical Infrastructure Protection. Do not include a full copy of your self-assessment.

Keep this Document

This is a working document. Its purpose is to start your process of security vulnerability assessment and security enhancements. Security is not an end point, but a goal that can be achieved only through continued efforts to assess and upgrade.

Don’t forget that this is a sensitive document. It should be stored separately in a secure place at your organization. A duplicate copy should also be retained at a secure off-site location. Access to this document should be limited to personnel, state and local officials, and others on a need-to-know basis.

Record of Security Vulnerability Self-Assessment Completion Form

The individual conducting the self-assessment and/or any additional revisions should complete the following information.

Name: ____

Title: ____

Area of Responsibility: ____

Company/Infrastructure: ____

Address: ____

City: ____

County: ____

State: ____

Zip Code: ____

Telephone: ____

Fax: ____

E-mail: ____

Date Completed: ____

Date Revised: Signature: ____

Date Revised: Signature: ____

Date Revised: Signature: ____

Date Revised: Signature: ____

Date Revised: Signature: ____

Executive Summary of the Security Vulnerability Self-Assessment

This executive summary outlines the business' primary mission and the critical assets or components to support the State of Utah or region's capability to provide continuity of operations, security, health and welfare of the citizens.

Business Name	
Business Address	
City, State, Zip Code	
Infrastructure Sector	
Primary Mission:	

Critical Assets or Components	Function

Emergency Contact Information: Identify three (3) independent departments within your business for emergency contact.

Name and Title or Department Name	Office Number	Mobile or Pager Number	Email

Certification of Security Vulnerability Self-Assessment Completion Form

A final step in completing the "Security Vulnerability Self-Assessment Guide is to notify the Utah Division of Homeland Security that the assessment has been conducted. To receive a certification of completion, please fill in the following information and **send this page only to Utah Division of Homeland Security Critical Infrastructure Protection**
1110 State Office Building, Salt Lake City, UT 84114 or by fax 801-538-3770

Company/Infrastructure: ____

Address: ____

City: ________________________**County**__________________

State: ________________________**Zip Code**_________________

Telephone: ________________________**Fax**_____________________

E-mail: ____

Contact (1) Name: ____

Title: ____

Telephone: ________________________**Fax**_____________________

E-mail: ____

Contact (2) Name: ____

Title: ____

E-mail: ____

Telephone: ________________________**Fax**_____________________

Contact (3) Name: ____

Title: ____

E-mail: ____

Telephone: ________________________**Fax**_____________________

Date Completed: ____

I certify that the information in this vulnerability self-assessment has been completed to the best of my knowledge and that the appropriate parties have been notified of the assessment and recommended steps to be taken to enhance the security of the infrastructure. Furthermore, a copy of the completed assessment will be retained at the organization, in a secure location, for state review as requested.

Signed_______________________________________**Date**____________________

Security Vulnerability Self-Assessment

General Questions for the Facility

The first 13 questions in this vulnerability self-assessment are general questions designed to apply to all components of your facility (buildings, equipment, storage areas, and equipment storage sites). These are followed by more specific questions that look at individual components in greater detail.

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
1. Do you have a written emergency response plan (ERP)?	Yes □ No □	It is essential that you have an ERP. If you do not have an ERP, you can obtain a sample from The Utah Division of Homeland Security. As a first step in developing your ERP, you should develop your Emergency Contact List (see Attachment 2). A plan is vital in case there is an incident that requires immediate response. Your plan should be reviewed at least annually (or more frequently if necessary) to ensure it is up-to-date and addresses security emergencies. You should designate someone to be contacted in case of emergency regardless of the day of the week or time of day. This contact information should be kept up-to-date and made available to your local police department, emergency personnel and local officials (if applicable). Share this ERP with police, emergency personnel, and DHS Posting contact information is a good idea only if authorized personnel are the only ones seeing the information. These signs could pose a security risk if posted for public viewing since it gives people information that could be used against the facility.	
2. Is access to the critical components of the facility (i.e., a part of the physical infrastructure of the facility that is essential for sensitive operations) restricted to authorized personnel only?	Yes □ No □	You should restrict or limit access to the critical components of your facility to authorized personnel only. This is the first step in security enhancement for your infrastructure. Consider the following: • Issue company photo identification cards for employees, and require them to be displayed within the restricted area at all times. • Post signs restricting entry to authorized personnel and ensure that assigned staff escort people without proper ID.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
3. Are facilities fenced, including warehouses and equipment yards and are gates locked where appropriate?	Yes □ No □	Ideally, all facilities should have a security fence around the perimeter. The fence perimeter should be walked periodically to check for breaches and maintenance needs. All gates should be locked with chains and a tamper-proof padlock that at a minimum protects the shank. Other barriers such as concrete "jersey" barriers should be considered to guard certain critical components from accidental or intentional vehicle intrusion.	
4. Are your doors, windows, and other points of entry such as roof hatches and vents kept closed and locked?	Yes □ No □	Lock all building doors and windows, hatches and vents, gates, and other points of entry to prevent access by unauthorized personnel. Check locks regularly. Dead bolt locks and lock guards provide a high level of security for the cost. A daily check of critical system components enhances security and ensures that an unauthorized entry has not taken place. Doors and hinges to critical facilities should be constructed of heavy-duty reinforced material. Hinges on all outside doors should be located on the inside. If unable to locate hinges on the inside of the building have the hinges been welded to prevent entry. Ensure all security enhancements meet the any fire code requirements. Alarms can also be installed on windows, doors, and other points of entry.	
5. Is there external lighting around the critical components of your facility?	Yes □ No □	Adequate lighting of the exterior of the facility's critical components is a good deterrent to unauthorized access and may result in the detection or deterrence of trespassers. Motion detectors that activate switches that turn lights on or trigger alarms also enhance security.	
6. Are warning signs (no trespassing, no unauthorized access, etc.) posted on all critical components of your facility?	Yes □ No □	Warning signs are an effective means to deter unauthorized access. "Warning - Tampering with this facility is a federal offense" "No Trespassing," "Authorized Personnel Only," "Unauthorized Access Prohibited," and "Employees Only" are examples of other signs that may be useful.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
7. Do you patrol and inspect your buildings, equipment, equipment storage sites, and other critical components?	Yes □ No □	Frequent and random patrolling your facilities staff may discourage potential tampering. It may also help identify problems that may have arisen since the previous patrol. Consider asking your local law enforcement agencies to conduct patrols of your facilities. Advise them of your critical components and explain why they are important.	
8. Is the area around the critical components of your facility free of objects that may be used for breaking and entering?	Yes □ No □	When assessing the area around your facility's critical components, look for objects that could be used to gain entry (e.g., vehicles, equipment, large rocks, cement blocks, pieces of wood, ladders, and other tools).	
9. Are the entry points to your facility easily seen?	Yes □ No □	You should clear fence lines of all vegetation. Overhanging or nearby trees may also provide easy access. Avoid landscaping that will permit trespassers to hide or conduct unnoticed suspicious activities. Trim trees and shrubs to enhance the visibility of your facility's critical components. If possible, park vehicles and equipment in places where they do not block the view of your critical components.	
10. Do you have an alarm system that will detect unauthorized entry or attempted entry at critical components?	Yes □ No □	Consider installing an alarm system that notifies the proper authorities or your facility's designated contact for emergencies when there has been a breach of security. Inexpensive systems are available and should be considered whenever possible for securing sensitive items. You should also have an audible alarm at the site as a deterrent and to notify neighbors of a potential threat.	
11. Do you have a key control and accountability policy?	Yes □ No □	Keep a record of locks and associated keys, and to whom the keys have been assigned. This record will facilitate lock replacement and key management (e.g., after employee turnover or loss of keys). Vehicle and building keys should be kept in a lockbox when not in use. Keep the key to the key box secure location not in the top drawer next to the key box. You should have all keys stamped (engraved) "DO NOT DUPLICATE."	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
12. Are entry codes and keys limited to company personnel only?	Yes □ No □	Suppliers and personnel from co-located organizations (e.g., organizations using your facility for telecommunications) should be denied access to codes and/or keys. Codes should be changed frequently if possible. Entry into any building should always be under the direct control of company personnel.	
13. Do you have a neighborhood watch program for your facility?	Yes □ No □	Watchful neighbors can be very helpful to a security program. Make sure they know whom to call in the event of an emergency or suspicious activity.	

Suppliers

Some facilities provide easy access for suppliers of equipment, chemicals, and other materials for the convenience of both parties. This practice should be discontinued.

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
14. Are deliveries of chemicals and other supplies made in the presence of company personnel?	Yes □ No □	Establish a policy that an authorized person, designated by the facility, must accompany all deliveries. Verify the credentials of all drivers. This prevents unauthorized personnel from having access to the facility.	
15. Have you discussed with your supplier(s) procedures to ensure the security of their products?	Yes □ No □	Verify that your suppliers take precautions to ensure that their products are not contaminated. Chain of custody procedures for delivery of chemicals should be reviewed. You should inspect chemicals and other supplies at the time of delivery to verify they are sealed and in unopened containers. Match all delivered goods with purchase orders to ensure that they were, in fact, ordered by your facility. You should keep a log or journal of deliveries. It should include the driver’s name (taken from the driver’s photo I.D.), date, time, material delivered, and the supplier’s name.	

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
16. Are chemicals, particularly those that are potentially hazardous or flammable, properly stored in a secure area?	Yes □ No □	All chemicals should be stored in an area designated for their storage only, and the area should be secure and access to the area restricted. Access to chemical storage should be available only to authorized employees. You should have tools and equipment on site (such as a fire extinguisher, drysweep, etc.) to take immediate actions when responding to an emergency.	

Personnel

You should add security procedures to your personnel policies.

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
17. When hiring personnel, do you request that local police perform a criminal background check, and do you verify employment eligibility (as required by the Immigration and Naturalization Service, Form I-9)?	Yes □ No □	It is good practice to have all job candidates fill out an employment application. You should verify professional references. Background checks conducted during the hiring process may prevent potential employee-related security issues. If you use contract personnel, check on the personnel practices of all providers to ensure that their hiring practices are consistent with good security practices.	
18. Are your personnel issued photo-identification cards?	Yes □ No □	For positive identification, all personnel should be issued company photo-identification cards and be required to display them at all times. Photo identification will also facilitate identification of authorized company personnel in the event of an emergency.	
19. When terminating employment, do you require employees to turn in photo IDs, keys, access codes, and other security-related items?	Yes □ No □	Former or disgruntled employees have knowledge about the operation of your company, and could have both the intent and physical capability to harm your facility. Requiring employees who will no longer be working at your company to turn in their IDs, keys, and access codes helps limit these types of security breaches.	

QUESTION	ANSWER	COMMENT	
20. Do you use uniforms and vehicles with your company name prominently displayed?	Yes □ No □	Requiring personnel to wear uniforms, and requiring that all vehicles prominently display the company name, helps inform the public when your staff is working. Any observed activity by personnel without uniforms should be regarded as suspicious. The public should be encouraged to report suspicious activity to law enforcement authorities.	
21. Have company personnel been advised to report security vulnerability concerns and to report suspicious activity?	Yes □ No □	Your personnel should be trained and knowledgeable about security issues at your facility, what to look for, and how to report any suspicious events or activity. Periodic meetings of authorized personnel should be held to discuss security issues.	
22. Do your personnel have a checklist to use for threats or suspicious calls or to report suspicious activity?	Yes □ No □	To properly document suspicious or threatening phone calls or reports of suspicious activity, a simple checklist can be used to record and report all pertinent information. Calls should be reported immediately to appropriate law enforcement officials. Checklists should be available at every telephone. Sample checklists are included in Attachment 3. Also consider installing caller ID on your telephone system to keep a record of incoming calls.	

Information storage/computers/maps

Security of your facility includes information storage, computers, facility maps goes beyond the physical aspects of your company. It also includes records and critical information that could be used by someone planning to disrupt or destroy your facility.

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
23. Is computer access “password protected?” Is virus protection installed and software upgraded regularly and are your virus definitions updated at least daily? Do you have Internet firewall software installed on your computer? Do you have a plan to back up your computers?	Yes □ No □	All computer access should be password protected. Passwords should be changed every 90 days and (as needed) following employee turnover. When possible, each individual should have a unique password that they do not share with others. If you have Internet access, a firewall protection program should be installed on your computer. Also consider contacting a virus protection company and subscribing to a virus update program to protect your records. Backing up computers regularly will help prevent the loss of data in the event that your computer is damaged or breaks. Backup copies of computer data should be made routinely and stored at a secure off-site location.	
24. Is there information on the Web that can be used to disrupt your facility?	Yes □ No □	Posting detailed information about your facility on a Web site may make your facility more vulnerable to attack. Web sites should be examined to determine whether they contain critical information that should be removed. You should do a Web search (using a search engine such as Google, Yahoo!, or Lycos) using key words related to your facility to find any published data on the Web that is easily accessible by someone who may want to damage your facility.	
25. Are maps, records, and other information stored in a secure location?	Yes □ No □	Records, maps, and other information should be stored in a secure location when not in use. Access should be limited to authorized personnel only. You should make back-up copies of all data and sensitive documents. These should be stored in a secure off-site location on a regular basis.	

QUESTION	ANSWER	COMMENT	
26. Are copies of records, maps, and other sensitive information labeled confidential, and are all copies controlled and returned to the company?	Yes □ No □	Sensitive documents (e.g., schematics, maps, and plans and specifications) distributed for construction projects or other uses should be recorded and recovered after use. You should discuss measures to safeguard your documents with bidders for new projects.	
27. Are vehicles locked and secured at all times?	Yes □ No □	Vehicles are essential to any company. They typically contain maps and other information about the operation of the facility. Company personnel should exercise caution to ensure that this information is secure. Company vehicles should be locked when they are not in use or left unattended. Remove any critical information about the company before parking vehicles for the night. Vehicles also usually contain tools that could be used to access your facility and are costly to replace. These tools should be secured and accounted for daily.	

Public Relations

You should educate your customers about your facility. You should encourage them to be alert and to report any suspicious activity to law enforcement authorities.

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
28. Do you have a program to educate and encourage the public to be vigilant and report suspicious activity to assist in the security protection of your company?	Yes □ No □	Advise your customers and the public that your company has increased preventive security measures to protect the facility from vandalism. Ask for their help. Provide customers with your telephone number and the telephone number of the local law enforcement authority so that they can report suspicious activities. The telephone number can be made available through direct mail, billing inserts, notices on community bulletin boards, flyers, and consumer confidence reports.	

QUESTION	ANSWER	COMMENT	
29. Does your facility have a procedure to deal with public information requests, and to restrict distribution of sensitive information?	Yes □ No □	You should have a procedure for personnel to follow when you receive an inquiry about the facility or its operation from the press, customers, or the general public. Your personnel should be advised not to speak to the media on behalf of the company. Only one person should be designated as the spokesperson for the company. Only that person should respond to media inquiries. You should establish a process for responding to inquiries from your customers and the general public.	
30. Do you have a procedure in place to receive notification of a suspected threat to your infrastructure?	Yes □ No □	It is critical to be able to receive information about suspected threats within your infrastructure at any time and respond to them quickly. Procedures should be developed in advance with your local, state, and federal agencies.	
31. Do you have a procedure in place to respond immediately to customer complaints?	Yes □ No □	It is critical to be able to respond to and quickly identify potential problems with customers. Procedures should be developed in advance to investigate and identify the complaint.	

Now that you have completed the “Security Vulnerability Self-Assessment,” review your needed actions and then prioritize them based on the most likely threats. A Table to assist you in prioritizing actions is provided in Attachment 1.

Attachment 1. Prioritization of Needed Actions

Once you have completed the "Security Vulnerability Self-Assessment," review the actions you need to take to improve your system's security. Note the questions to which you answered "no" on this worksheet. You can use it to summarize the areas where your system has vulnerability concerns. It can also help you prioritize the actions you should take to protect your facility from vulnerabilities. Make sure to prioritize your actions based on the most likely threats to your facility.

Question Number	Needed Action	Scheduled Completion

Attachment 2. Emergency Contact List

We urge all critical infrastructures to adopt an emergency response plan (ERP). Emergency response plans are action steps to follow if the infrastructure is compromised or if the service is disrupted. You can obtain sample ERPs from the Division of Homeland Security.

This sample document is an “Emergency Contact List.” It is an essential part of your ERP. It contains the names and telephone numbers of people you might need to call in the event of an emergency. This is a critical document to have at your disposal at all times. It gives you a quick reference to all names and telephone numbers that you need for support in the case of an emergency.

Filling out this Emergency Contact List reminds you to think about all of the people you might need to contact in an emergency. It also may encourage you to talk with these people about what you and they would do if an emergency were to occur.

Section 1. Company/Infrastructure Information

Company/Infrastructure Name		
Company/Infrastructure Address		
City, State, Zip Code		
Telephone Numbers	Main Number	Evening/Weekend Number
Other Contact Numbers	Main Fax	Email
Population Served and Number of Service Connections	People Served	Connections
Name, title, and telephone number of person responsible for company/infrastructure security	Name and Title	Home Number
		Office Number
	Email	Cellular Number
		Pager Number
Name, title, and telephone number of person responsible for maintaining this emergency contact list	Name and Title	Home Number
		Office Number
	Email	Cellular Number
		Pager Number

Section 2. Notification / Contact Information

Local Notification List

ORGANIZATION	CONTACT NAME / TITLE	TELEPHONE (DAY)	TELEPHONE (NIGHT)	EMAIL
Homeland Security	Critical Infrastructure / Liaison	(801) 538-3400		www.des.utah.gov
Utah Highway Patrol				
Police Department				
Sheriff’s Office				
FBI Field Office				
Fire Department				
Local HAZMAT Team				
EMS				
Federal Regulating Department				
State Regulating Department				
Local Government Official				
Local Emergency Manager				
Local Emergency Planning Committee				
Local Hospital				
Local Schools				
Neighborhood Watch Program				
Other				

Service / Repair Notification List

ORGANIZATION	CONTACT NAME / TITLE	TELEPHONE (DAY)	TELEPHONE (NIGHT)	EMAIL
Security / Alarm Company				
Electric Utility Company				
Gas Utility Company				
Sewer Utility Company				
Telephone Utility Company				
Computer Specialist				
Construction Contractor				
Electrical Contractor				
Plumbing Contactor				
Local Disaster Cleanup Specialist				
Blue Stakes				
Equipment Rental				

State Notification List

ORGANIZATION	CONTACT NAME / TITLE	TELEPHONE (DAY)	TELEPHONE (NIGHT)	EMAIL
Utah Division of Homeland Security	Renee Murphy, Program Manager or CI Staff	(801) 538-3702 (801) 538-3400	(801) 718-3124	rmurphy@utah.gov
National Guard		(801) 523-4400		
Department of Commerce		(801) 530-6446		www.commerce.utah.gov
Department of Environmental Quality		(801) 536-4400		www.deq.utah.gov
Department of Health		(801) 538-6101		www.doh.utah.gov
Labor Commission		(801) 530-6800		www.laborcommission.utah.gov
Department of Natural Resources		(801) 538-7200		www.nr.utah.gov

Media Notification List

ORGANIZATION	CONTACT NAME / TITLE	TELEPHONE (DAY)	TELEPHONE (NIGHT)	EMAIL
Designated Media Spokesperson				
Newspaper – Local				
Newspaper – Regional/State				
Radio				
Radio				
Radio				
Television				
Television				
Television				

Section 3. Communication and Outreach

Communication

Communications during an emergency can create special problems. A standard response in an emergency is to call “911” for local fire and police departments. But what if the emergency has disrupted telephone lines and over-loaded cell phone lines? Talk with the Division of Homeland Security and your state-regulating department about local emergency preparedness and solutions to these problems. Increasingly, state emergency agencies are establishing secure lines of communication with limited access. Learn how you can access those lines of communication if all others fail.

Outreach

If there is an incident that the infrastructure is compromised or if the service is disrupted, you will need to notify Emergency Services and make recommendations for continuity of service. To do this, you need a plan.

□ How will you reach all customers in the first 24 hours of an emergency?

□ Appoint a media spokesperson—a single person designated who will be authorized to make all public statements to the media.

□ Make arrangements for contacting institutions with large numbers of people that may be adversely affected by the disruption:

- Nursing homes
- Hospitals
- Schools
- Prisons

Attachment 3: Threat Identification Checklists

Telephone Threat Identification Checklist

In the event that the infrastructure receives a threatening phone call, remain calm and try to keep the caller on the line. Use the following checklist to collect as much detail as possible about the nature of the threat and the description of the caller. The bomb threat identification checklist can also be used for other potential threats. (See FBI Bomb Card)

QUESTIONS TO ASK **EXACT WORDING OF THREAT**

1. When is the bomb going to explode? ____
2. Where is it right now? ____
3. What does it look like? ____
4. What kind of a bomb is it? ____
5. What will cause it to explode? ____
6. Did you place the bomb? ____
7. Why? ____
8. What is your address? ____
9. What is your name? ____

Note if (and how) the caller seems familiar with the building by description of bomb location.

EXACT WORDING OF THE THREAT

____

____

____

____

____

____

Sex of caller __________ Age __________ Ethnicity__________

Time call received __________ Time call hung up __________

Caller ID number ___________ Connection (Land line or cellular phone) __________

Fill out completely, immediately following the bomb threat. Check all that apply.

CALLER'S VOICE

□ Calm

□ Angry

□ Excited

□ Slow

□ Rapid

□ Soft

□ Intoxicated

□ Laughing

□ Crying

□ Normal

□ Distinct

□ Slurred

□ Nasal

□ Loud

□ Lisp

□ Raspy

□ Deep

□ Ragged

□ Clearing Throat

□ Deep Breathing

□Stutter

□ Disguised

□ Whispered

□ Cracking Voice

□ Accent
*Nationality?*__ __________

□ Familiar
*If voice is familiar, who did it sound like?*_________________

THREAT LANGUAGE

□ Well Spoken (*Educated)*

□ Taped

□ Foul

□ Message read by threat marker

□ Irrational

□ Incoherent

BACKGROUND SOUNDS

□ Street Noises ____

□ Voices (Adults/Children) ____

□ Animal Noises ____

□ Music ____

□ House Noises ____

□ Office Noises ____

□ Machinery (Office/Factory) ____

□ Motors ____

□ Other ____

Call Received By __________________________ Date ___________ Time ___________

Telephone Number ________________ Position _______________ Department ____________

Call Reported To __________________________ Date ___________ Time ___________

Report of Suspicious Activity Checklist

In the event personnel from your infrastructure or neighbors observe suspicious activity, use the following checklist to collect as much detail about the nature of the activity.

1. Types of Suspicious Activity:

□ Breach of Security (e.g. lock cut, door forced open)

□ Unauthorized personnel on property

□ Presence of personnel at location at unusual hours

□ Person Taking Pictures

□ Unusual Information Requests

□ Suspicion of Surveillance

□ Other (Explain)____

____

2. Location of Suspicious Activity:

□ Office □ Plant □ Equipment Yard □ Warehouse

□ Construction Site □ Off Site Location________________________________

□ Other (Explain)____

3. Description of Events:

What made the activity suspicious____

____

Breach of security (Specify nature and location)______________________________

____

What made the person suspicious____

____

What made the vehicle suspicious____

____

4. Description of Person:

Name____________________ Sex____________ Age________________

Address____

Telephone________________ DL Number_______ Ethnicity____________

Height___________________ Weight__________ Hair Color___________

Distinguishing Marks_________ Clothes__________ Facial Hair__________

5. Vehicle Information:

Make_____________________ Model_______________ Type_______________

License Plate_______________ State________________ Color_______________

Number of Passengers_______ Year_________________

Distinguishing Marks (e.g. dents, stickers)____

6. Report Prepared By (Name, Department, and Telephone Number):

Date of Incident:________________ Time of Incident:__________________

7. Incident Reported to:______________________ Date/Time:________________

8. Action(s) Taken Following Receipt of the Report:

Disclaimer

This document contains information on how to plan for protection of the assets of your infrastructure. The work necessarily addresses problems in a general nature. You should review local, state, and federal laws and regulations to see how they apply to your specific situation. Knowledgeable professionals prepared this document using current information. The authors make no representation, expressed or implied, that this information is suitable for any specific situation. The authors have no obligation to update this work or to make notification of any changes in statutes, regulations, information, or programs described in this document. Publication of this document does not replace the duty of the organization to warn and properly train their employees and others concerning health and safety risks and necessary precautions at their infrastructures. Neither the Utah Division of Homeland Security, Association of State Drinking Water Administrators, the National Rural Water Association, the U. S. Environmental Protection Agency, the Drinking Water Academy, nor its contractor, The Cadmus Group, Inc., assume any liability resulting from the use or reliance upon any information, guidance, suggestions, conclusions, or opinions contained in this document.

Acknowledgments

This document was developed from the Association of State Drinking Water Administrators (ASDWA), and the National Rural Water Association (NRWA) Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems. We also thank NWRA for the template that was used as the foundation for this project.